International Research Journal of Rongo University (IJORU) ISSN: 3005-7221
Transformative Research and Innovation for an Inclusive and Sustainable Future
Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

SOCIAL MEDIA AND INSECURITY: A CRITICAL REVIEW OF YOUTH PLATFORM EXPLOITATION AND PERSONAL SECURITY THREATS IN KISII COUNTY

[1]Migiro Gilbert Ombasa*, [1]Fredrick Ogenga, [1]Henry Kinya

*Corresponding Author: gilbertmigiro@yahoo.com

https://orcid.org/0009-0000-4541-1303; https://orcid.org/0000-0002-0044-3296; https://orcid.org/0009-0004-5257-1670

[1]Rongo University, P.O. Box 103-40404 Rongo, Kenya

Abstract

The rapid proliferation of social media has transformed communication patterns among youth, offering unprecedented opportunities for interaction, information sharing, and self-expression. However, these digital platforms have also introduced significant personal security threats. This paper examines the nature, extent, and implications of social media-related security risks facing youths in Kisii County, Kenya. Drawing from existing literature, empirical studies, and contextual analysis, the study identifies key threats including exposure to harmful content, online fraud, identity theft, surveillance, and cyberbullying as the most prevalent social media security threat affecting youths in Kisii County. This study is grounded in Routine Activity Theory (RAT). The paper further explores the socio-cultural and technological factors that heighten youth vulnerability and proposes strategic interventions grounded in digital literacy, policy enforcement, and stakeholder collaboration. The study adopted a qualitative research design that integrated multiple complementary approaches to ensure depth and contextual relevance. It involved a systematic document analysis of scholarly articles, policy reports, and institutional publications to establish a strong theoretical and empirical foundation. In addition, a contextual analysis centered on Kisii County was undertaken to ground the study within its specific socio-cultural and geographical setting. The findings highlight the urgent need for integrated approaches to safeguard youth in an increasingly digitized environment.

Keywords: *social media, youth, personal security, cybercrime, Kisii County, Kenya*

Introduction

The integration of digital technologies into everyday life has significantly transformed patterns of communication, particularly among young people. All over the world, social media provides communication among young people through chatting they can connect with friends. Video calls have also provided wider avenues for interaction among young people and have also been an avenue for security breaches (Tufekci, 2018). The influence of social media on youths is especially profound since most of them use smartphones and other devices to stay connected (Ingutia, 2025). Social networking sites provide avenues for social interaction, knowledge-sharing, and creativity, while also enabling peer learning through collaboration on projects. Additionally, social media offers valuable resources for teens seeking health information, connecting with support networks, or exploring personal identity. However, the risks associated with social media, such as cyberbullying, exposure to inappropriate content, and online harassment, cannot be ignored. These dangers can result in serious psychological consequences, including depression, anxiety, and even suicide (Wandhe, 2024).

In Kenya, increased smartphone penetration and affordable internet access have accelerated social media adoption, especially among youths. Despite these advantages, the digital landscape presents significant risks. Social media environments often expose young users to various personal security threats, including cyberbullying, online fraud, and identity theft (Livingstone & Smith, 2014). In Kisii County, where

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

digital adoption is rapidly increasing, many youths lack the skills and awareness necessary to navigate online risks effectively. This study aimed at examining the nature of social media-related personal security threats facing youths in Kisii County, identify contributing factors, and propose strategies to enhance online safety.

There are many various types of social media platforms available currently, both independent and interconnected, making it challenging to define social media (Kemp, 2023). Users' contributions, whether in the form of digital photos or videos, postings or comments, or information compiled from all online interactions, are what provide life and vitality to social media platforms (Abdirahman, 2023). Social media platforms such as Facebook, WhatsApp, Instagram, TikTok, and X (formerly Twitter) have become central to youth interaction, enabling real-time communication, networking, and content sharing. Social media crimes are becoming increasingly more common with issues such as data breaches more prominent. Social networking platforms such as Facebook, Twitter, Instagram, and Snapchat have become integral to people's social interactions, with many freely expressing their updates and viewpoints (Kemp, 2023). The cyber-crime incidences of spear phishing are also on the increase and involve the installation of harmful malware on the computer or device and stealing valuable and sensitive information (Moore, 2020).

Abdirahman (2023) assert that social media is a double-edged sword. The use of social media can either perpetuate or prevent crime in society. In this era of social media, government security agencies have adopted the use of social media to investigate, prevent and deal with crime. Social media pose threats due to social and economic challenges. Ingutia (2025) notes that the increased availability of new technologies has resulted in a rise in cyber bullying cases in recent years. As a member of the international community, Kenya is not immune to social media forces. It is prone to the misuse of social media by users. The use of the platforms on social media poses huge security concerns for the nation and its citizens.

Research on use of social media suggests that social uses top the list such as exchanging of emails and chatting, the highest percentage of people have email accounts (Nishad, 2018). Cyber criminals send emails with the motive of defrauding their victims or invite them for a false interview that the that the mainstream organisation knows nothing about. Some go as far as collecting application fee from unsuspecting job seekers to be recruited (Hufnagel et al., 2019). A good deal of research has found that social media influences security (Gupta et al., 2018; Walsh, 2020; Walsh & O'Connor, 2019; Zhang & Gupta, 2018). According to Gupta et al. (2018), criminals use social media platforms to perpetrate crimes and violence to their target victims based on their online activities. Cyber criminals target social media sites by use of malware programs aimed at a computer or a network (Walsh, 2020; Zhang & Gupta, 2018). Studies carried out show that social media users or someone they know has experienced online romance scams with the users forging new relationships online (De Jong, 2019). Loneliness has been attributed to victims who get involved in online romance scams a study carried out shows that most victims are females (Shaari et al., 2019).

Though the reviewed literature link social media use to security, it fails to focus on the youth and fails to address personal security. The review literature does not address the influence of social media on protection from physical violence, domestic violence, exploitation and scams that are aspects of personal security. All these studies focus on various social media crimes and threats to security. The problem is that the reviewed studies do not clearly address relationship between different forms of social media and personal security. There is therefore need to establish how different aspects of personal security are influenced by various forms of social media. This study is grounded in Routine Activity Theory. Routine Activity Theory (RAT) was developed by Cohen and Felson (1979), it posits that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in time and space. It focuses on how daily routines and environmental opportunities, rather than offender motivations alone, drive crime rates. That crime is not solely the result of offender motivation or social pathology but emerges from routine patterns of legitimate activities that shape criminal opportunities.

Methodology

Research methodology is the theoretical perspective of the research, that is, the overall nature of the research

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

activity. The study adopted a qualitative research design that integrated multiple complementary approaches to ensure depth and contextual relevance. It involved a systematic document analysis of scholarly articles, policy reports, and institutional publications to establish a strong theoretical and empirical foundation. This method also allows researchers to gain deep insights into how the topic under study has evolved over time, as well as how concepts and understandings of the topic have changed over the years (Neuendorf, 2018). In this research, it is important to scrutinise the reliability and credibility of the sources used, as well as critically analyse the information collected. The focus of a qualitative literature review is to collate, evaluate and integrate existing knowledge on the topic under study. One of the advantages of a qualitative literature review is its flexibility in understanding and explaining complex phenomena, as it is not limited by numerical or statistical constraints (Babbie, 2010).

Contextual analysis is the process of interpreting data (which may include textual, visual, or auditory), language or behavior by considering the surrounding context rather than looking at information in isolation (Conner et al., 2012). In addition, a contextual analysis centered on Kisii County was undertaken to ground the study within its specific socio-cultural and geographical setting. To enrich the analysis further, a comparative review of regional and global studies on youth and digital security was conducted, allowing for broader insights and cross-contextual understanding. Collectively, these approaches facilitated a comprehensive synthesis of existing knowledge pertinent to the study.

Results and Discussions

Prevalent Social Media Security Threats

Cyberbullying

The results indicate that cyberbullying is one of the most pervasive social media security threats affecting youths in Kisii County. This form of online aggression manifests through multiple channels, including hostile or demeaning comments on public posts, abusive private messages, and the circulation of humiliating or defamatory content within peer networks. Social media platforms such as Facebook, WhatsApp, Instagram, and TikTok were identified as the primary spaces where such interactions occur, largely due to their high usage among young people and their affordances for rapid content sharing and anonymity

Reviewed content indicated that cyberbullying often takes the form of name calling, body shaming, spreading of rumours, and targeted harassment based on personal characteristics such as appearance, academic performance, or socio-economic status. In some cases, the bullying extended to the non-consensual sharing of personal images or screenshots of private conversations, amplifying the victim's exposure and vulnerability. The persistence and visibility of online content were noted to intensify the impact of such attacks, as harmful messages can be repeatedly accessed, shared, and commented on by wider audiences (Evans, 2023).

The psychological and emotional consequences of cyberbullying emerged as significant. Victims frequently described experiences of anxiety, stress, low self-esteem, and, in severe cases, symptoms associated with depression. The reputational damage caused by public humiliation was also highlighted, particularly within tightly knit community and school environments where online interactions often intersect with offline relationships. This dual exposure; online and offline, exacerbates the social consequences, making it difficult for victims to escape the effects of bullying (Dharejo et al, 2023). Moreover, the study found that many youths lack adequate coping mechanisms or institutional support systems to address cyberbullying. While some participants reported blocking perpetrators or withdrawing from social media platforms, others remained silent due to fear of escalation or stigmatization. The limited involvement of parents, educators, and local authorities in monitoring and addressing online behavior further compounds the problem (Barati, 2023).

These findings are consistent with the work of Kowalski et al. (2014), who established that cyberbullying is associated with adverse emotional and psychological outcomes among adolescents. The Kisii County context reinforces the global understanding of cyberbullying while also highlighting unique local dynamics, such as strong peer influence and the blending of digital and physical social spaces. Consequently, addressing cyberbullying requires not only technological

interventions but also community-based awareness, digital literacy education, and strengthened policy enforcement mechanisms to protect young social media users.

Online Fraud

The study established that online fraud is a significant and growing threat to youths in Kisii County, driven largely by increased digital engagement and economic vulnerability. The analyzed policy reports showed that frequent exposure to fraudulent schemes on popular platforms such as Facebook, WhatsApp, Telegram, and Instagram, where scammers exploit the informal and trust-based nature of online interactions. These schemes commonly take the form of fake online businesses, deceptive job offers, scholarship scams, and impersonation of trusted individuals or institutions.

A recurring pattern involves fraudulent online businesses advertising attractive products such as electronics, clothing, or mobile phones. These are at unusually low prices. Youths are often required to make advance payments via mobile money services, particularly M-Pesa, only for the seller to disappear or deliver substandard or entirely different goods. Similarly, fake job advertisements promising quick employment or high returns require applicants to pay "facilitation fees," registration charges, or training costs, which ultimately result in financial loss without any legitimate opportunity materializing (Oblad, 2021).

The findings further indicate that the economic circumstances of many youths heighten their susceptibility to such scams. High levels of unemployment and underemployment in the region create a sense of urgency and optimism that fraudsters exploit. As Leukfeldt (2014) suggests, individuals facing financial constraints are more likely to engage with risky online opportunities, especially when they appear to offer quick financial relief. In Kisii County, this vulnerability is compounded by limited digital literacy, making it difficult for some youths to critically evaluate the authenticity of online offers. Another emerging dimension of online fraud involves social engineering tactics, where scammers manipulate victims psychologically rather than technically (Abdirahman, 2023). For instance, perpetrators may hack or clone social media accounts and use them to request money from the victim's contacts, leveraging existing trust relationships. In other cases, phishing messages disguised as official communication from banks, mobile service providers, or government agencies are used to extract sensitive information such as passwords, PINs, or one-time verification codes.

These findings align with broader research on cybercrime, which highlights how socio-economic vulnerability, combined with low awareness of cybersecurity practices, increases the likelihood of victimization (Leukfeldt, 2014). Within the Kisii County context, the prevalence of mobile money usage and the rapid adoption of social media platforms create an enabling environment for fraudsters. Addressing this challenge therefore requires targeted interventions, including digital literacy campaigns, public awareness initiatives on common scam tactics, and stronger regulatory frameworks to monitor and respond to online fraud.

Identity Theft

The study findings reveal that identity theft is an increasingly prevalent risk among youths in Kisii County, largely driven by the culture of oversharing personal information on social media platforms. Many young users routinely disclose sensitive details such as full names, dates of birth, phone numbers, school affiliations, locations, and even personal identification documents through posts, profiles, or public interactions. While often shared for social visibility and peer engagement, this information creates a digital footprint that can be easily exploited by malicious actors.

The study found that social media profiles frequently contain enough aggregated data to enable impersonation and fraudulent activities. Perpetrators can use publicly available information to create fake accounts that closely resemble those of legitimate users, thereby deceiving friends, family members, and broader networks. In some cases, scammers clone entire profiles replicating photos, bios, and friend lists and then use these accounts to solicit money, spread misinformation, or engage in further cybercrimes under the victim's identity.

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

Data showed instances where personal information shared online was used to bypass basic security verification systems, particularly in mobile money and online service platforms. For example, knowledge of a person's full name, phone number, and social connections can be sufficient for social engineering attacks, enabling fraudsters to manipulate customer care agents or reset account credentials. This highlights the intersection between identity theft and other forms of cybercrime, such as online fraud and phishing.

A major contributing factor identified in the study is limited awareness of privacy settings and digital security practices. Many youths either lack knowledge of how to restrict access to their profiles or underestimate the risks associated with making personal information publicly accessible (Chang et al., 2023). Additionally, the desire for social validation manifested through frequent posting and engagement; often outweighs concerns about privacy and security.

The obvious consequences of identity theft are multifaceted. Victims may suffer financial losses, reputational damage, and psychological distress, particularly when their identities are used to defraud others or circulate harmful content. In tightly knit communities such as those in Kisii County, such incidents can have far-reaching social implications, affecting trust and interpersonal relationships both online and offline. Moreover, the process of reclaiming one's digital identity such as reporting fake accounts or restoring compromised profiles can be complex and time-consuming, with limited institutional support available at the local level.

The above study findings are consistent with Reyns et al. (2011), who argue that the accessibility of personal information on social networking sites significantly increases the risk of identity theft. The Kisii County context reinforces this perspective by demonstrating how socio-cultural practices, combined with technological exposure, contribute to vulnerability. Addressing identity theft therefore requires a multifaceted approach, including enhanced digital literacy education, promotion of responsible online self-disclosure, and stronger platform-level protections to safeguard user identities.

Privacy Violations and Surveillance

Reviewed content indicated that many youths are unaware of privacy settings and data tracking mechanisms. This lack of awareness increases exposure to exploitation and surveillance according to (Zuboff, 2019).

Harmful Content Exposure

The study found that exposure to harmful content is a significant and often under-recognized risk affecting youths in Kisii County. With increased access to smartphones and affordable internet, young users are routinely exposed to a wide range of online material, including violent imagery, sexually explicit content, hate speech, and misleading or manipulative information. Social media platforms such as Facebook, TikTok, YouTube, and WhatsApp were identified as key channels through which such content circulates, often amplified by algorithm-driven recommendations and peer sharing. It was also found out that harmful content is frequently encountered both intentionally and unintentionally. While some youths actively seek out sensational or trending material, many reported accidental exposure through auto-play features, shared links in group chats, or platform suggestions based on prior engagement. This blurring of intentional and unintentional consumption makes it difficult for users to control the type and volume of content they encounter.

The findings suggest that repeated exposure to violent and explicit material can desensitize youths, normalizing aggression, risky sexual behavior, and other socially undesirable practices. In addition, misleading content, particularly in the form of misinformation and disinformation, was found to shape perceptions, attitudes, and decision-making processes. For instance, false narratives related to health, politics, or social issues can influence beliefs and behaviors in ways that may be harmful both to individuals and the wider community. Youths in the study also reported psychological and emotional effects associated with harmful content exposure, including fear, anxiety, confusion, and moral conflict. Younger and more impressionable users were particularly vulnerable, as they often lack the critical media literacy skills needed to interpret and evaluate online content effectively. The absence of consistent

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

parental guidance and limited institutional regulation further exacerbates this vulnerability (Kemp, 2023).

Moreover, the study highlights the role of peer networks in reinforcing exposure. Content shared within trusted social circles tends to be perceived as credible, even when it is harmful or misleading. This peer validation can accelerate the spread of problematic content and deepen its impact. In some cases, social pressure encourages continued engagement with such material, as youths seek to remain socially relevant or entertained.

These findings align with UNICEF (2021), which emphasizes that exposure to harmful online content can significantly influence young people's cognitive, emotional, and behavioural development. In the context of Kisii County, the convergence of high social media usage, limited digital literacy, and evolving cultural norms creates a complex environment where harmful content can thrive.

Factors Contributing to Youth Vulnerability

The study identified several interrelated factors that heighten the vulnerability of youths in Kisii County to social media related security threats. These factors operate at individual, social, economic, and institutional levels, collectively shaping how young people engage with digital platforms and the risks they encounter. Among the most prominent factors is low digital literacy. Many youths possess basic operational skills for using smartphones and social media applications but lack critical knowledge of online safety practices, such as privacy management, secure password use, and the ability to identify scams or misleading content. This gap leaves them ill-equipped to navigate complex digital environments safely. As noted by Mutua (2020), limited digital literacy significantly increases susceptibility to cyber threats, as users are less likely to recognize or respond appropriately to online risks.

Peer influence also emerged as a powerful driver of vulnerability. Social media engagement among youths is heavily shaped by the desire for social validation, acceptance, and belonging. This often leads to conformity with peer norms, including participation in risky online behaviors such as oversharing personal information, engaging with strangers, or joining trending but potentially harmful online challenges. Drawing on the work of Boyd (2014), the findings underscore how networked publics create environments where visibility and validation become central, sometimes at the expense of personal safety and privacy.

Economic constraints further exacerbate vulnerability. High levels of youth unemployment and financial instability in Kisii County push many young people to seek opportunities online, including jobs, business ventures, and financial investments. In this context, the urgency to secure income often overrides caution, making youths more prone to falling victim to online fraud, scams, and exploitative schemes. The promise of quick financial gain becomes particularly appealing, even when warning signs are present.

Another critical factor is weak enforcement of cybercrime laws. Although legal frameworks to address cybercrime exist in Kenya, their implementation at the local level remains inconsistent and, in some cases, ineffective. Participants expressed limited confidence in reporting mechanisms and law enforcement responses, which discourages victims from seeking help and allows perpetrators to operate with relative impunity. This institutional gap contributes to a broader environment where online offenses are normalized or go unpunished.

Finally, the study highlights the challenge of technological access without corresponding education. The rapid proliferation of affordable smartphones and internet connectivity has significantly increased youths' access to digital platforms. However, this access has not been matched with adequate training or awareness programs on responsible and safe usage. As a result, many youths engage with advanced technologies without a foundational understanding of the associated risks, creating a mismatch between access and preparedness. In combination, these factors create a layered vulnerability framework in which individual limitations, social dynamics, economic pressures, and institutional weaknesses intersect. Addressing youth vulnerability in Kisii County therefore requires a holistic approach that integrates digital literacy education, socio-economic empowerment, stronger policy enforcement, and community-based awareness initiatives.

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

Implications

The findings of this study point to far-reaching implications that extend beyond individual experiences to affect families, communities, and broader societal systems in Kisii County. These implications underscore the urgency of addressing social media related security threats among youths through coordinated and multi-level interventions. A major implication is the rise in mental health challenges among young people. Exposure to cyberbullying, online harassment, identity theft, and harmful content contributes to psychological distress, including anxiety, depression, and, in some cases, trauma. The persistent and public nature of online interactions intensifies these effects, as victims often feel unable to escape or control their digital environments. Over time, this can undermine self-esteem, academic performance, and overall well-being, highlighting the need for integrating mental health support into digital safety initiatives.

Economic losses also emerged as a critical consequence. Many youths fall victim to online fraud, resulting in direct financial exploitation through scams such as fake businesses, fraudulent job offers, and phishing schemes. For individuals already facing economic constraints, these losses can be devastating, reinforcing cycles of financial insecurity and limiting opportunities for economic advancement. Additionally, repeated exposure to fraud may discourage youths from engaging in legitimate digital economic activities, thereby hindering participation in the growing digital economy. The study further reveals significant social disruption arising from these threats. Incidents such as cyberbullying, impersonation, and misinformation erode trust among peers, families, and communities. Relationships are strained when individuals are deceived, publicly humiliated, or falsely represented online. In tightly knit social settings like those in Kisii County, the overlap between online and offline interactions amplifies these tensions, leading to conflicts, social withdrawal, and, in some cases, long-term reputational damage.

Another important implication is the potential increase in cybercrime within the broader community. As more youths are exposed to and, in some instances, inadvertently learn from online fraudulent practices, there is a risk of normalization and replication of such behaviors. This creates a cycle in which victims may become perpetrators, contributing to the expansion of cybercrime networks. The cumulative effect is a deterioration of digital security at the community level, posing challenges for law enforcement and governance structures. Overall, these implications demonstrate that social media security threats are not isolated issues but interconnected challenges with psychological, economic, and social dimensions. Addressing them requires comprehensive strategies that combine digital literacy, mental health support, economic empowerment, and strengthened legal and institutional frameworks to foster a safer digital environment for youths

Conclusion

Social media has become an indispensable tool for youth engagement in Kisii County, shaping communication, access to information, and socio-economic participation. However, as this study demonstrates, its benefits are accompanied by significant personal security challenges that cannot be overlooked. From cyberbullying and online fraud to identity theft and exposure to harmful content, the risks facing young users are multifaceted and deeply embedded in both technological and socio-cultural contexts. The findings highlight the complexity of these threats, showing that they are driven not only by individual behaviors but also by broader structural factors such as limited digital literacy, economic vulnerability, peer influence, and weak enforcement of cybercrime regulations. This interplay of factors underscores the need for responses that go beyond isolated interventions and instead adopt a comprehensive, systems-based approach. Addressing these challenges requires integrated strategies that combine digital literacy education, stronger policy implementation, and active stakeholder collaboration. Educational institutions must play a central role in equipping youths with critical skills for safe online engagement, while policymakers and law enforcement agencies need to strengthen the enforcement of existing cyber laws. At the same time, parents, community leaders, and technology companies must work collaboratively to create supportive and secure digital environments. Ultimately, protecting youths in digital spaces is not merely a technological concern but a social

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

imperative. Ensuring their safety online is essential for fostering trust, resilience, and meaningful participation in the digital age. By prioritizing coordinated and sustained interventions, stakeholders can help build a safer, more inclusive digital future for young people in Kisii County and beyond.

Recommendations

Digital Literacy Education

Integrate digital safety into school curricula and community programs to enhance awareness and resilience. Educating youths about the dangers of social media use is vital. Education should commence within families, spread to communities and schools, and encompass government-led activities such as online conferences, seminars, or workshops aimed at youths. Educating members of society is necessary to counteract the spread of false information and fake news on social media. When people read something online, they should be more critical of what they read and should question material that is consistent with their values. The creation of a digital environment that is more trustworthy and secure can be accomplished through the promotion of critical thinking and accountability online.

Strengthening Policy Enforcement

Enhance the implementation of Kenya's Computer Misuse and Cybercrimes Act (2018) to deter cyber offenses. There is need to translate the Computer Misuse and Cybercrimes Act, 2018, and the Data Protection Act, 2019, into easily understandable, actionable guides for the public. The government of Kenya and regulatory organisations should prioritise the development of cyber policies, the enforcement of regulations, and the implementation of tighter data protection legislation as the impact of cyber crime on social media becomes increasingly apparent in society. In addition, individuals who do not comply with the policies, laws, and regulations pertaining to cyberspace should be subject to sanctions.

Multi-Stakeholder Collaboration

Encourage partnerships among government agencies, educational institutions, parents and technology companies. To effectively combat cybercrime on social media, it is necessary for individuals, organisations, social media platforms, and service providers to work together. Through the strengthening of defences, the raising of awareness, and the comprehension of the vulnerabilities that exist in social media, we can build a more secure environment online. To be successful, the battle against cybercrime on social media platforms is an ongoing process that calls for continuous collaboration, creativity, and a commitment to making cyber security a top priority in the digital age.

Youth Empowerment Programs

Promote responsible digital citizenship and critical thinking skills. A greater number of programs and initiatives should be implemented to give work chances for young people and persons who are currently without jobs in Kenya. This would help address the problem of unemployment and social media crime in the country. It is possible for individuals to gain financial and mental stability through the creation of additional employment options, which in turn reduces the possibility that they will engage in criminal activities.

Platform Accountability

Social media companies should improve privacy protections, reporting systems, and content moderation. There should be strict penalties for individuals and organizations that generate or disseminate harmful content, including hate speech, sexually explicit material, fraudulent religious activities etc. Social media platforms should also be encouraged to use artificial intelligence and machine learning algorithms to filter and block inappropriate content before it spreads widely. For purposes of identifying potential dangers, cyber intelligence is an essential component of cyber security. In addition, cyber threat intelligence can be utilised for incident response by delivering information that can be put into action during security incidents.

Declaration of generative AI and AI-assisted technologies in the writing process

The authors, while preparing this work, utilized ChatGPT for spellchecking and grammar refinement. The work was then carefully reviewed and edited as necessary and assumes full responsibility for the publication's content.

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

Declaration of funding sources

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. We conducted this study independently, without external financial support, to contribute to academic knowledge in the field of technology.

Credit authorship contribution statement

Migiro: Writing – review & editing, Conceptualization, Methodology, Software, Visualization, Investigation, Validation, Writing-original draft preparation, Data curation. **Ogenga:** Writing -review & editing, Visualization, Supervision. Validation **Kinya:** Writing - review & editing, Visualization, Supervision, Validation.

Declaration of conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this research. We have no financial or personal relationships with any individuals or organizations that could inappropriately influence or bias the content of this work. Our primary objective is to contribute to scholarly discourse and advance knowledge in the field without any competing interests.

Acknowledgement

I extend my sincere gratitude to my supervisors, Prof. Fredrick Ogenga and Dr. Henry Kinya, for their invaluable guidance, support, and mentorship throughout the research process. Their expertise, insightful feedback, and encouragement have been instrumental in shaping this study and enhancing its quality. I am deeply grateful for their unwavering dedication and commitment to excellence. We owe much thanks to International Research Journal of Rongo University for accepting making our work known to the world of academia.

References

Abdirahman, I. (2023). Exploring Co-Regulation as a Solution to Automated Disinformation in Kenya. *Journal of Intellectual Property and Information Technology Law (JIPIT), 3*(1), 201–256. https://doi.org/10.52907/jipit.v3i1.262

Babbie, E. (2010). *The practice of social research* (12th ed.). Belmont, CA: Wadsworth.

Barati, M. (2023). Casual social media use among the youth: Effects on political participation. *JeDEM - eJournal of eDemocracy and Open Government, 15*(1), 1–21. https://doi.org/10.29379/jedem.v15i1.738

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Calbalhin, J. P. (2018). Facebook User's Data Security and Awareness: A Literature Review. *Journal of Academic Research, 2*(June 2018), 1–13.

Chang, W., & Chang, H. (2023). The impact of digital disruption: influences of digital media and social networks on forming digital natives, attitude. *Sage Open, 13*(3), 1–10. https://doi.org/10.1177/21582440231191741

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Communications Authority of *Kenya. (2020). Fourth Quarter Sector Statistics Report for the Financial Year 2019/20 (April-June 2020).* https://www.ca.go.ke/sites/default/files/2023-06/Sector%20Statistics%20Report%20Q4%202019-2020.pdf

Conner, F., Fitzpatrick, L., & Rog, J. (2012). A first step forward: Context assessment. *New Directions for Evaluation, 2012*(135), 89–105. https://doi.org/10.1002/ev.20029

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology, 58*(6), 1303– 1322.

De Jong, K. (2019). *Detecting the online romance scam: Recognising images used in fraudulent dating profiles* [Master's thesis, University of Twente]. https://essay.utwente.nl/80084/1/Jong_de_MA_EEMCS.pdf

Dhami, A., Aggarwal, N., Chakraborty, K., Singh, P., & Minj, J. (2013). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. In 2013 3rd

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

IEEE International Advance Computing Conference (IACC) (pp. 465–469). IEEE. https://doi.org/10.1109/IAdCC.2013.6514270

Dharejo, N., Alivi, M., Rahamad, S., Jiaqing, X., & Brony, M. (2023). Effects of social media use on adolescent psychological well-being: A Systematic literature review. *International Journal of Interactive Mobile Technologies, 17*(20), 171–191.

Elsaesser, C. M., Patton, D. U., Kelley, A., Santiago, J., & Clarke, A. (2021). Avoiding fights on social media: Strategies youth leverage to navigate conflict in a digital era. *Journal of Community Psychology, 49*(3), 806–821.

Evans, O. (2023). Connecting the poor: the internet, mobile phones and financial inclusion in Africa. *Digital Policy, Regulation and Governance, 20*(6), 568-581.

Government of Kenya. (2018). *Computer misuse and cybercrimes act*. Government Printer.

Gupta, S. S., Thakral, A., & Choudhury, T. (2018). Social media security analysis of threats and security measures. In *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)* (pp. 115–120). IEEE. https://doi.org/10.1109/ICACCE.2018.8441710

Ingutia, B. (2025). The impact of social media in shaping Kenya's politics: Gen Z uprising and the rejection of the Finance Bill 2024. *African Multidisciplinary Journal of Research, 1*(1), 47–68.

Jude, A. V., & Pdmakumari, P. (2025). Social media activism: Delving into Generation Z's experiences. *Communication Research & Practice, 12*(1), 20–37. https://doi.org/10.1080/22041451.2025.2554375

Kemp, S. (2023, February 13). *Digital 2023: Ken*ya. DataReportal. https://datareportal.com/reports/digital-2023-kenya

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age. *Psychological Bulletin, 140*(4), 1073–1137.

Leukfeldt, R. (2014). Phishing for suitable targets. *Crime Science, 3*(1), 1–13.

Livingstone, S., & Smith, P. (2014). Harms experienced by child users of online technologies. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654.

Makinde, O. A., Olamijuwon, E., Ichegbo, N. K., Onyemelukwe, C., & Ilesanmi, M. G. (2021). The nature of technology-facilitated violence and abuse among young adults in sub-Saharan Africa. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald international handbook of technology facilitated violence and abuse* (pp. 83–101). Emerald Group Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211005

Manyerere, D. J. (2021). Youth Perceptions, Use and Effects of Social Media on Peace and Conflicts in Tanzania. *Ghana Journal of Development Studies, 18*(2), 48–73.

Moore, K. (2020). *The Use and Effectiveness of Law Enforcement Social Media Sites*. University of Oklahoma, SHAREOK Institutional Repository.

Mutua, J. (2020). Cybersecurity awareness among Kenyan youth. *African Journal of Information Systems, 12*(3), 45–60.

Neuendorf, K. A. (2018). Content analysis and thematic analysis. In P. Brough (Ed.), *Advanced research methods for applied psychology* (pp. 211-223). Routledge.

Nilan, P., Burgess, H., Hobbs, M., Threadgold, S., & Alexander, W. (2015). Youth, Social Media, and Cyberbullying Among Australian Youth: "Sick Friends." *Social Media and Society, 1*(2), 1–12. https://doi.org/10.1177/2056305115604848

Oblad, T. (2021). Understanding self-harm and coping among minority youth. *International Journal of Scientific Academic Research,* 2(1), 736-738.

Received 13/07/2026; Revised 09/08/2026; Accepted 05/10/2026

Ogenga, F. (2024). '*Kenya's Twin Burden: Balancing the Security of Tech Infrastructure Against its Role in Online Extremism*'. Global Network on Extremism and Technology (GNET).

Radcliffe, D., & Bruni, P. (2019). State of social media, Middle East: 2018. Radunović, V., & Veinović, M. (2020). Malware command and control over social media: Towards the server-less infrastructure. *Serbian Journal of Electrical Engineering, 17*(3), 357–375. https://doi.org/10.2298/SJEE2003357R

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online. *Crime & Delinquency, 57*(4), 578–600.

Shaari, A. H., Kamaluddin, M. R., Paiz Fauzi, W. F., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies, 19*(1), 97–115.

Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2008). Cyberbullying research. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385.

Tamori, A., Bhujade, R. K., Sinhal, A., & Professor, A. (2018). Analysis on WhatsApp Security. *International Journal of Ethics in Engineering & Management Education, 5*(6), 1–4. https://www.researchgate.net/publication/328048673_Analysis_on_WhatsApp_Security

Tufekci, Z. (2018). *How social media took us from Tahrir Square to Donald Trump*. MIT Technology Review. https://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump

UNICEF. (2021). *Children in a digital world*. UNICEF.

United Nations Population Fund. (2025). *Adolescent and youth dashboard*. https://www.unfpa.org/data/KE

Waechter, N. (2021). Gendered social media cultures between individuality and collectively. In *Forms of Collective Engagement in Youth Transitions* (pp. 185-206). Brill. https://doi.org/10.1163/9789004466340_010

Wandhe, P. (2024). *The new generation: understanding millennials and Gen Z*. SSRN. https://doi.org/10.2139/ssrn.4716585

Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs.